

Privacy Act

(Compliance Training)

United States Army

Overview

This training applies to the Privacy officials, system owners, program managers, and all other individuals who are responsible for fulfilling the requirements of the Privacy Act.

This training covers:

- The publication of Privacy Act System of Record Notices (SORN)
- Handling and reporting of personally identifiable information (PII) incidents
- The uses of social security numbers (SSN)

What is PII?

Personally Identifiable Information (PII) is defined as: Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, DOD ID, biometric records alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, and so forth. ([OMB M-07-16](#))

Overview



After completion of this training, you should be familiar with:

- Ways of Embedding Privacy Into Information Systems
- Privacy Compliance Requirements
- Breach Management
- SSN Reduction

Embedding Privacy into Information Systems

The Privacy Act requires agencies to adopt . . .

*“appropriate **administrative, technical** and **physical** safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity . . .”*



Embedding Privacy into Information Systems

Whenever a Federal agency maintains information about an individual in an information technology (IT) system or paper file system and retrieves the information by a personal identifier, it must publish a System of Records Notice (SORN) in the Federal Register.

The following slides outline the Privacy compliance process in publishing a System of Records Notice.

Privacy Compliance

When developing or procuring new IT systems that will collect and store Personally Identifiable Information (PII):

- System Owners, Program Managers, and Information Assurance (IA) staff should be aware of and understand the Department of Defense's Risk Management Framework (RMF) Assessment and Authorization (A&A) process.
- RMF A&A is a process by which information systems are certified for compliance with DoD security requirements and accredited for operation by a designated official.

Privacy Compliance



RMF A&A process provides visibility and control for the secure operation of DoD's information systems. RMF considers the:

- mission or business need
- protection of personally identifiable information
- protection of the information being processed
- protection of the systems information environment

Privacy Compliance

The compliance process begins with the **Privacy Threshold Analysis (PTA)**.

The purpose of the PTA is to:

- Identify systems that are privacy-sensitive.
- Demonstrate the inclusion of privacy considerations during the review of a system.
- Provide a record of the system and its privacy requirements.

The PTA tells whether a system has privacy relevance, and if additional privacy compliance documentation is required, such as a **Privacy Impact Assessment (PIA)** and **System of Records Notice**.

Privacy Compliance

A **Privacy Impact Assessment** is a decision-making tool used to analyze how information is handled. The purpose of the PIA is to:

1. Identify and mitigate privacy risks at the beginning of and throughout the development life cycle of a system.
2. Determines the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and
3. Examines and evaluate protections and alternative processes to mitigate potential privacy risks.



Privacy Compliance

If a PIA is required, the program manager or system owner should prepare and submit a PIA package to Chief Information Officer (CIO G6).

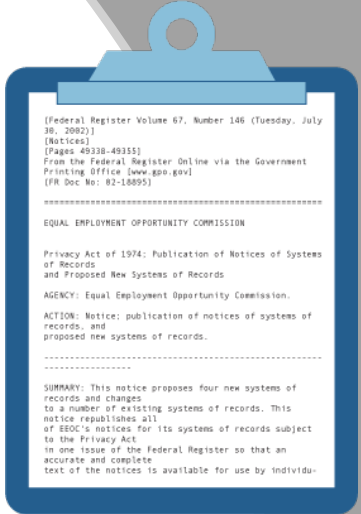
Note: The PTA and PIA process only applies to IT systems, not paper files.

For step-by-step guidance on completion of a PTA and PIA, refer to ciog6.army.mil.

Privacy Compliance

A **System of Records** is a group of records from which information is retrieved by a unique personal identifier (i.e., name, SSN, etc.) assigned to an individual.

A **System of Records Notice** is a formal notice to the public published in the Federal Register that identifies the purpose for which PII is collected, from whom, what type, how information is shared, and how to access and correct information maintained by the agency.



[Federal Register Volume 67, Number 146 (Tuesday, July 30, 2002)]
[Notices]
[Pages 49338-49355]
From the Federal Register Online via the Government
Printing Office [www.gpo.gov]
[FR Doc No: 02-18095]

=====

EQUAL EMPLOYMENT OPPORTUNITY COMMISSION

Privacy Act of 1974: Publication of Notices of Systems of Records and Proposed New Systems of Records

AGENCY: Equal Employment Opportunity Commission.

ACTION: Notice; publication of notices of systems of records, and proposed new systems of records.

SUMMARY: This notice proposes four new systems of records and changes to a number of existing systems of records. This notice republishes all of EEOC's notices for its systems of records subject to the Privacy Act. In one issue of the Federal Register so that an accurate and complete text of the notices is available for use by individuals.

Privacy Compliance

The following guidelines should be followed when drafting a SORN.

- **Remember the audience.** The SORN should be written in a manner that allows the public to understand the records being described.
- **Use plain English.** Use words, phrases, or names in the SORN that are readily known to the average person.
- **Explain acronyms.** Spell out each acronym the first time it is used in the document. Do not use acronyms in the summary of the notice.
- **Correct simple errors.** This document is meant to be published in the Federal Register.

Privacy Compliance

- **Define technical terms or reference.** Keep in mind that readers may not understand technical terms when they are introduced without definition.
- **Cite legal references and other previously published documents.** Reference other programs and systems and provide explanations so that the general public can gain a complete understanding of the context of the program or system.
- **Use the complete name of reference documents.** For example: National Institute of Science and Technology (NIST) *Special Publications 800-26, and Security Self-Assessment Guide for Information Technology Systems.*

Privacy Compliance



- An Office of Management and Budget (OMB) Control Number may be required before implementation of a system of records collection.
- If collecting information from ten or more people of the general public, you must follow the guidelines of the Paperwork Reduction Act 44 U.S.C. § 3501-352. OMB assigns control numbers for information collection requirements.
- For additional information on the Paperwork Reduction Act refer to the [Paperwork Reduction.gov](https://www.paperworkreduction.gov) website.

Privacy Compliance

- **ALL** SORNs are approved by the Defense Privacy and Civil Liberties Office (DPCLO) prior to publication.
- SORNs are sent to OMB and to Congress for comment and then published in the Federal Register for thirty days.
- A system may not become operational until the SORN has been published.
- A complete listing of Army SORNs is located on [DPCLO's website](#).

Privacy Compliance

Agencies are required to provide a **Privacy Act Statement (PAS)** to all persons asked to provide personal information about themselves.

PAS allows the individual to make an informed decision about providing his or her data.

PAS is required when an individual is asked to:

- provide his or her SSN or other personal data.
- confirm that his or her information is current.

A PAS is required regardless of whether the collection is part of a system of records or not.

For additional information, refer to [DoD 5400.11-R](#)



Privacy Compliance

The PAS tells the individual:

The legal **authority** for collecting the information.

The **purpose** for collecting the information and how it will be used.

The **routine uses** that apply to the data and the Army organization.

The **disclosure** of information and whether it is mandatory or voluntary and the effect(s), if any, of not providing the information. For example, the loss or denial of a privilege, benefit, or entitlement.

Privacy Compliance

Various information collection devices exist. Some examples include:

- Information Systems
- Forms
- Surveys & Questionnaires
- Web Sites
- Verbal Questions



Privacy Compliance

The following are examples of where to place a Privacy Act Statement.

- Immediately under the title of the form
- Elsewhere on the front page of the form (clearly indicating it is the PAS)
- On the back of the form with a notation of its location before the title of the form
- On a separate sheet which the individual may keep.

Surveys:

- Opening page of survey or in a cover memo appended to the survey.

Web Pages:

- Conspicuously on the screen that collects the data.

A sample form with a Privacy Act Statement at the top. The statement is in a red box and reads: "I have read and understand the purpose of this form and the information that will be collected and how it will be used. I agree to provide the information requested and to allow the collection and use of my information for the purposes stated." Below the statement is a line for a signature and a line for a date. The form is titled "LOREM IPSUM DOLOR SIT AMET" and contains several sections of text and lines for input.

FORMS

A sample survey form with a Privacy Act Statement at the top. The statement is in a red box and reads: "I have read and understand the purpose of this survey and the information that will be collected and how it will be used. I agree to provide the information requested and to allow the collection and use of my information for the purposes stated." Below the statement is a line for a signature and a line for a date. The form is titled "LOREM IPSUM DOLOR SIT AMET" and contains several sections of text and lines for input.

SURVEYS

A sample web page with a Privacy Act Statement at the top. The statement is in a red box and reads: "I have read and understand the purpose of this web page and the information that will be collected and how it will be used. I agree to provide the information requested and to allow the collection and use of my information for the purposes stated." Below the statement is a line for a signature and a line for a date. The web page is titled "LOREM IPSUM DOLOR SIT AMET" and contains several sections of text and lines for input.

WEB PAGES

Privacy Compliance



Before development of a paper file or IT system, you should:

- Check whether a SORN has been published covering your collection.
- Verify that the data elements are covered in the system of records notice.
- Consult with your local Privacy Office.

Breach Management

The Army continues to implement policies and practices to safeguard the PII of its personnel and their families. Part of this process is to properly report the suspected or actual loss of this information and to notify those impacted.

A breach is the:

- actual or possible loss of control of personally identifiable information; or
- unauthorized disclosure or access of personally identifiable information.

Breach Management

If you can answer “YES” to any of the following questions, you have a reportable breach.

- Has data been lost?
- Has data been stolen?
- Has data been compromised?



Breach Management



All Army Commands, ARMY Service Component Commands, Direct Reporting Units, Army Staff, Program Executive Offices, and agencies will ensure reporting and notification occur in accordance with the following procedures.

Breach Management

When data maintained by Army personnel or contractors is lost, stolen, or compromised:

- Immediately notify your Command Privacy Officer.
- Report the incident to the United States Computer Emergency Readiness Team (US-CERT) (within 1 hour).
- Report the incident to Army Privacy Office (within 24 hours).
The reporting format and submission guidelines are located on the Records Management and Declassification Agency (RMDA) [website](#).
- Submit updated reports reflecting the results of the investigative efforts, remedial action and notification efforts as they become available.

Breach Management

- The Army Privacy Office is the centralized office for all Army PII incident reporting, information, and statistics.
- Continue to follow existing internal command procedures to notify local command officials.
- The organization responsible for safeguarding the PII at the time of the incident is responsible for notifying the affected individuals.
- The decision about whether to notify individuals rests with the Head of the Army command where the breach occurred.

Breach Management

The following are examples of harm to an individual as result of a breach:

- Identity theft
- Discrimination
- Emotional distress
- Inappropriate denial of benefits
- Harm to reputation
- Blackmail
- Embarrassment



Breach Management



There are five factors you should weigh when analyzing a breach:

- How the loss occurred.
- Nature of data elements breached and number of individuals affected.
- Ability and likelihood that the information is accessible and useful.
- Ability of the agency to mitigate the risk of harm.

Breach Management

Elements of Notification: if it is determined that notification is necessary, include the following elements:

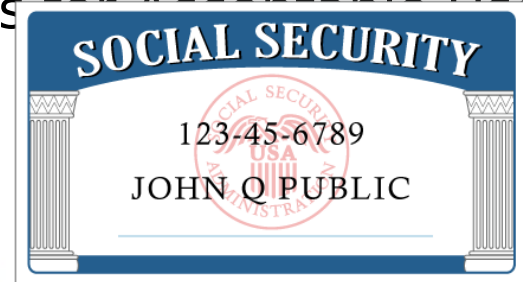
- A description of the specific data involved
- Facts and circumstances surrounding the loss, theft, or compromise
- A statement regarding if and how the data was protected (e.g., encryption)
- Any mitigation support services
- Protective actions that are being taken or other actions the individual can take to protect themselves against future harm
- Provide a point of contact for more information

Social Security Number Reductions

Are you aware of the DoD's policy to reduce or eliminate the use of SSNs?

In April 2007, the President's Task Force on Identity Theft issued a strategic plan which required that every agency develop and implement a plan to reduce the unnecessary use of SSNs

DoD Guidance (DoDI 1000.30) lists 13 cases for Acceptable Uses of SSNs. System owners, in consultation with their Privacy Official, must ensure that IT system that collects, maintains, uses, or disseminates SSNs have written justification for continued use.



Social Security Number Reductions



SSN has been used as a means to efficiently identify and authenticate individuals.

Expanded use of the SSN has increased efficiency, enabling systems and process to interoperate and transfer information with reduced errors.

However, the threat of identity theft has rendered this use unacceptable, requiring all Federal agencies to evaluate how the SSN is used and eliminate its unnecessary use.

Social Security Number Reductions

The acceptable uses of the SSN are those:

- Provided by law
- Requiring interoperability with organizations beyond the agency
- Required by operational necessities, i.e. inability to alter systems, processes, forms due to cost or unacceptable levels of risk

Note: claims of operational necessities are closely scrutinized. Ease of use or unwillingness to change are not acceptable justifications.

References

DoDI 8510.01- “Risk Management Framework (RMF) for DoD Information Technology

Defense Privacy and Civil Liberties Office –

<http://dpclo.defense.gov>

Army Regulation 340-21, “The Army Privacy Program”

DoD Directive 5400.11, “DoD Privacy Program”

DoD Regulation 5400.11-R, “Department of Defense Privacy Program”

DA&M Memorandum, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”

